7. Withstanding the Storm: Digital Silk Road, Covid-19 and Europe's Options

Tyson Barker

In April 2016, President Xi captured China's sense of technological vulnerability in an arresting way:

> Our dependence on core technology is the biggest hidden trouble for us. Therefore, having a good command of core Internet technology is our mission. Heavy dependence on imported core technology is like building our house on top of someone else's walls: No matter how big and how beautiful it is, it won't remain standing during a storm.[1]

By that point, the logic of Xi's statement had informed China's pursuit of cyber sovereignty – through fits and starts – for the better part of two decades. But as China's capacity to produce core Internet and Communication Technology (ICT) hardware, effectively regulate Internet traffic and transform its ICT and digital services have grown, Beijing's Digital Grand Strategy, itself, has shifted – from a feature of the country's domestic development to a frontline domain in the global race for technological leadership and a key vector in the export of China's model of authoritarianism.

[1] CRI Online, "Core technology depends on one's own efforts: President Xi", *People's Daily Online*, 19 April 2018.

In the eyes of the Chinese Communist Party (CCP), the Covid-19 crisis has in many ways vindicated its model of development. The crisis exacerbated political fissures in the US; economic stagnation in Europe and Japan; and debt-reliance in the Global South – all the while, fuelling a massive acceleration in global technological adoption. China posted 2.3% growth in 2020. China's 14th Five-Year Plan seems to indicate that the country withstood the Covid-19 storm.[2] It also seems to show that the Covid-19 crisis has, in many ways, validated China's methodical quest for cyber sovereignty, rooted in state control that intermediates technologically-enabled social relationships at home, as well as China's broad technological connective tissue with the outside world through the Digital Silk Road (DSR).

The Covid-19 crisis has validated China's methodical quest for cyber sovereignty, rooted in state control that intermediates technologically-enabled social relationships at home, as well as China's broad technological connective tissue with the outside world through the Digital Silk Road

The first post-Covid Five-Year Plan envisions China continuing to move up the food chain of advanced research, through progress in the following 7 "frontiers of science and technology": 1) next-generation AI; 2) quantum technology; 3) integrated circuits; 4) brain research and neural networks; 5) genetics and biotechnology; 6) clinical medicine and health; and 7) exploration of space, the deep layers of the earth, the deep sea and the polar regions.[3] The 192-chapter plan – which shifts the focus away from GDP growth targets and towards consolidated power and global leadership – also recasts national security in terms that extend the logic of end-to-end control beyond technology, to areas like food, finance and energy.

[2] GT staff reporters, "China's 5-year plan to lead global recovery", *Global Times*, 8 March 2021.

[3] Bundesverband der Deutschen Industrie e.V. (BDI), *Nationaler Volkskongress: Arbeitsbericht der Regierung*, National People's Congress, Government Work Report, 9 March 2021.

At the heart of China's Covid-19 strategic shift is the "dual circulation" model, unveiled by President Xi in September 2020.[4] Under this model, China aims to use the DSR to push forward with global technological integration on Chinese terms, while inoculating itself against external technological dependencies. This, of course, is set against the backdrop of 3 geopolitical realities that could pose headwinds to the DSR's post-Covid development. First, the increasingly sophisticated American approach to US-China strategic competition under the Biden Administration, which is now couched in the language of multilateralism and increasingly embedded in a network of allies. Second, global collapse of trust in China due to its opacity around the Covid outbreak and its aggressive "wolf warrior" diplomacy, particularly during the first wave, combined with deteriorating fiscal conditions in partner countries. And finally, an ambivalent Europe, whose economic dependence on China accelerated during the crisis, but whose political orientation is simultaneously more suspicious of China's intentions and more rooted in its own aspirations for digital sovereignty.

This chapter attempts to provide a topography of the DSR during the Covid-19 crisis and what it means in a global context, particularly for the European Union. In order to do so, the piece first examines the primary elements of technological development in China, which serve as the domestic basis for the country's "going out" strategy in the ICT arena. The second section examines the slow yet steady rise within the Belt and Road Initiative (BRI) of its digital connectivity pillar, the DSR with its emphasis on ICT infrastructure, technology and digital services. The third section looks at the changes in emphasis that

Under the dual circulation model, China aims to use the DSR to push forward with global technological integration on Chinese terms, while inoculating itself against external technological dependencies

[4] K. Yao, "What we know about China's 'dual circulation' economic strategy", *Reuters*, 15 September 2020.

have characterised some areas of the DSR's Covid era evolution, namely the growing role of digital services, greater use of mergers and acquisitions, an increased focus on the domestic market focus as part of a "reverse-flow" DSR, and new emphasis on regulatory mirroring and global governance. The final section concludes with a consideration of the potential blind spots of the EU, as it grapples with the logic of the DSR at home and globally. This essay does not aspire to provide exhaustive analysis of the next chapter of the DSR, not least because the geopolitical and economic conditions shaping China's Geotech ambitions necessitate constant recalibration. It does, however, attempt to capture the intellectual foundation – and its features – upon which Beijing has structured its quest to build a digital hub-and-spoke system on a global scale.

Broad Political Elements of Chinese Technology Development

Over recent decades, China's domestic technological modernisation had been characterised by four key elements, all of which interact with China's internationalisation efforts. First, it has long used a form of import substitution in the digital sector to harness the power of its indigenous market to incubate local players. The Great Chinese Firewall – and legal restrictions on foreign operations of many digital services like Facebook and Google within China – have created a protected single market of 802 million Internet users. That has provided fertile ground for scalable growth and an accommodating market. Even if competition among Chinese tech companies in areas like AI, platform provision and e-commerce can be ferocious, it is relatively sheltered from the asymmetric degree of competition that international competitors would have provided.

The centrality of the domestic market remains an important, although changing feature of China's tech foreign policy. Even though China has 111 Fortune 500 companies – a fifth of the

global total – over 80% of their business is done domestically.[5] Despite advances in technological research in frontier areas like artificial intelligence and telecommunications equipment, China continues to be a global taker of intellectual property (IP) – the primary basis for technological development – importing 6 times more global IP than it creates. That asymmetric relationship is highly concentrated. A majority of China's tech IP imports stem from just 3 countries: the US (31%), Japan (21%) and Germany (10%).[6] As such, cyber economic espionage, once called the greatest wealth transfer to China in the history of the world, continues and has increased in sophistication. IP theft and other forms of tech transfer are at the root of some of China's most successful tech companies, such as Qihoo, Meituan, Dianping and SMIC.

Second, the relationship between the state and Chinese enterprises does not reflect the independent and, at times, deeply antagonistic behaviour between democracies on the one hand and their private sector on the other. The intermediation role of the state – and of the Chinese Communist Party in particular – governing and legitimising all social and commercial encounters cannot be overstated. The PRC's constitution "prohibits any organisation or individual to damage the socialist system" rooted in the legitimising wellspring of the CCP.[7]

This logic of state/CCP intermediation and control extends to the digital sphere. The de facto fusion of state and enterprise into a single vertical entity takes different forms, from state-owned enterprises, to the structure of management boards and the legal overhang granted by broadly-worded statutes, such as the sweeping data localisation requirement that "important

[5] J. Woetzel et al., *China and the world: Inside the dynamics of a changing relationship*, McKinsey Global Institute, July 2019, p. 29.

[6] Ibid., p. 3.

[7] D.K. Tatlow, "China's Technological Rise. Implications for Global Security and the Case of Nuctech", Rahvusvaheline Kaitseuuringute Keskus (RKK), International Centre for Defence and Security (ICDS), and Estonian Foreign Policy Institute (EVI), January 2021, p. 2.

data" must be stored in accordance with the 2017 Cyber Security Law. The 2017 National Intelligence Law contains blanket mandates for "all organisations and citizens" to support national intelligence efforts (Art. 7) and grants China's intelligence services authority to request support (Art. 14).

In the past, the government has effectively conscripted Chinese tech companies to render data collection, surveillance and processing for government use. Frequently, individual Chinese IT specialists and even Chinese companies are forced into a relationship with the government, under which they are required to perform services around data collection and processing. In combination with the increasing development of enabling, general-purpose technologies and the fusion of China's innovative industrial base with its military, China's tech industry is becoming a core component of the People's Liberation Army's (PLA) modernisation and range of capabilities.

Third – and this is connected with the fusion of state and enterprise – are the governing principles of Chinese ICT development. At their heart, these are rooted in the notion of "social harmony", with its communitarian basis, where state control is legitimised by creating a harmonious society through a strict hierarchical order.[8] The second-order principles – sovereignty, opacity, a perceived justification of end-to-end surveillance as a "public good", the de-emphasis of human rights, unlimited data availability and non-individual control – reinforce the bond between the state/CCP, telecommunications state-owned enterprises (SOEs), state adjacent tech champions and start-ups. Grafted together by state investment, procurement structures that advantage state-favored companies, forced joint ventures and sharing of technology IP gathered through state-backed industrial espionage with copy-cat companies at home. This co-dependence, with the state/CCP as the undisputed senior partner, is a hallmark of China's domestic technology and

[8] *NextGen Network: How AI Can Work for Humanity*, The Aspen Institute, 18 November 2020.

digital services market. Failure to adhere to the arrangement can have serious consequences.[9] At the same time, China has instrumentalised key technologies to enforce its authoritarian governance model through industrial-grade AI-surveillance, suppression and control at home, particularly in areas of political unrest like Xinjiang and Hong Kong.[10]

Fourth – and flowing from the first three elements – is the consistent state ambition to control technical standards both domestically and internationally. These aims have been expressed over the years but often been blocked due to lack of control over external technological ecosystems and capacity within the global technical standard setting community. In 2004, for instance, China's attempt to establish an autarkic national wireless LAN authentication and privacy infrastructure (WAPI) ran into massive pushback among China's IT sector and the international community because it was feared that the rival standard to the internationally recognised WLAN would create another cleavage between the Chinese national Internet and its global counterpart. Amid mounting pressure, and in view of the collateral damage the WAPI standard would have done to the competitiveness of Chinese IT, Beijing ultimately backed down from the WAPI standard.

TD-SCDMA (Time Division Synchronous Code Division Multiple Access) is another example. TD-SCDMA was China's attempt at developing the leading standards for 3G mobile, developed in conjunction with the German industrial conglomerate, Siemens.[11] China Mobile was forced into accepting the exclusive rights from the Chinese government in 2009, despite its desire to use the more globally interoperable

[9] In the first 3 weeks of 2019, the Chinese government shutdown 700 websites and 9000 mobile apps. A. Polyakova and C. Meserole, *Exporting digital authoritarianism*, Brookings, August 2019.

[10] K. Sahin et al., *The West, China, and AI Surveillance*, Atlantic Council, 18 December 2020.

[11] "China's 3G Technology Gamble: Who Has the Last Laugh?", *Knowledge@Wharton*, Wharton University of Pennsilvanya, 6 July 2011.

Wideband Code Division Multiple Access (WCDMA). But because it was air-gapped from the global standard, developers were less interested in developing hardware and services for China's autarkic standard. As a result, the perception in 2011 was that the telecoms market remains beholden to foreign technology. Ultimately, China Mobile was allowed to pull the plug on TD-SCDMA in favour of the more interoperable TD-LTE 4G in 2014, after having invested more than US$32 billion in network infrastructure.[12] In 2011, only 7% of China's mobile users were on 3G systems, as opposed to 100% of Japanese users, 47% of Europeans and 40% of Americans.[13] Today the adoption picture is different. Across a number of areas – such as 5G connectivity, health tech, mobile payments and digital currency – China is a leader in adoption and is now positioned as a standard setter.

As China's homegrown R&D, ICT production overcapacity and indigenous capabilities have increased – particularly in AI, connectivity hardware, and increasingly platforms and fintech – it has moved some of its tech champions up the ranks of global competitiveness

As China's homegrown R&D, ICT production overcapacity and indigenous capabilities have increased – particularly in AI, connectivity hardware, and increasingly platforms and fintech – it has moved some of its tech champions up the ranks of global competitiveness. Chinese tech champions have begun to aggressively internationalise and diversify – including Huawei and ZTE in its first wave. Alibaba aims to generate 40% of its revenue from outside China by 2027 and have 1 out of 2 billion net buyers located outside China by 2036. China's more robust ICT "going out" strategy has been a particular driver of new frictions with the United States, which has recognised the geostrategic implications. Between 2017 and early 2020, the US scaled up the use of the Entity List, which forbids the

[12] S. Kinney, "RIP: China Mobile's TD-SCDMA 3G network (2009-2014)", *RCR Wireless News*, 14 December 2014.

[13] "China's 3G Technology Gamble: Who Has the Last Laugh?"…, cit.

export and IP usage of American technology by named Chinese companies, and doubled the number of CFIUS (Committee on Foriegn Investment in the United States) investigations.[14] In response, China has pointed to its own ICT supply chain choke-holds on rare earths[15], cobalt[16] and even essential patents for 5G technology, and has hinted at a possible willingness to exploit them.

The DSR in the Context of the Belt and Road Initiative

China's digital development began to attract greater global attention around 2015, following the launch of the Made in China 2025 (MiC2025) plan, which outlines a 10-year industrial policy aimed at transforming 10 core industries into world leaders in their respective sectors. The plan was updated in 2017, with a closer focus on domestic autonomy in key emerging technologies. Its Internet+ subset outlined the intention to integrate manufacturing and services with digital technology more fully by design. The 13th Five-Year Plan included specific GDP and R&D targets, with a view to powering economic growth through innovation. It was followed by China's 2016 AI Strategy and China Standards 2035, each citing specific targets, as well as industrial and capacity resources, with an eye to Chinese technological leadership.

The DSR as an app plug-in for the BRI

The Digital Silk Road (2015) draws on three core state-driven strategies: Made in China 2025, the Belt and Road Initiative and China Standards 2035. The DSR integrates all three, while

[14] From 73 annually under Obama to 147 under Trump.

[15] Yun Li, "'Don't say we didn't warn you': A phrase from China signals the trade war could get even worse", *CNBC*, 29 May 2019.

[16] L.Ch. Savage, "How America got outmaneuvered in a critical mining race", *Politico*, 12 February 2020.

simultaneously seeking to generate network effects for the competitiveness of China's ICT stack; creating new markets and digital service relationships to the Middle Kingdom, and export Chinese industry standards in next-generation technologies.[17] Over 6000 tech enterprises are registered on the BRI Portal and over one third of Chinese FDI in BRI countries is in technology areas.

Over 6000 tech enterprises are registered on the BRI Portal and over one third of Chinese FDI in BRI countries is in technology areas

The BRI combines the land-based economic belt, made up of 6 development corridors, with the XXI century maritime silk road. The initiative names 5 key priorities: 1) policy coordination, 2) infrastructure connectivity, 3) unimpeded trade, 4) financial integration, and 5) connecting people. The initiative is funded by a mix of Chinese state-owned and state-controlled banks and funds, as well as a number of international finance institutions (IFIs), including the Asia Development Bank and European Bank for Reconstruction and Development (EBRD).[18] As of January 2021, China has signed BRI Memoranda of Understanding (MoUs) with 140 countries, including 34 in Europe and Central Asia and, by Chinese accounts, 18 EU countries (although many of these dispute or have not confirmed their formal participation).[19]

DSR projects were initially perceived as primarily plug-in projects to core BRI projects in rail, maritime and road infrastructure. The BRI model is a highly integrated infrastructure ecosystem that links ports to research parks and cities. This pairs connectivity along transport infrastructure with more specific AI-surveillance and security monitoring at stations, ports and shipping and storage facilities. It also allows

[17] J.E. Hillman, *Competing with China's Digital Silk Road*, Center for Strategic & International Studies, 9 February 2021.

[18] *The EBRD and BRI*, European Bank for Reconstruction and Development, 2021.

[19] *Countries of the Belt and Road Initiative (BRI)*, Green Belt and Road Initiative Center, January 2021.

for latent control over a broader infrastructure ecosystem that can make the recipient country susceptible to normative influence in benign times, extract concessions in competitive times or be weaponised at times of hostility.

The defining feature of the DSR, however, has been its core focus on connectivity infrastructure, both in telecommunications/5G hardware and smart cities. Most attention in Europe has therefore centred on equipment sourcing for core and radio access network (RAN) 5G infrastructure from Huawei and ZTE. Together Huawei and ZTE account for 38% of the global mobile equipment market.[20] An aggressive push for external market share in partner countries has been aided by two factors: first, the relatively low cost of Chinese technologies, particularly telecommunications equipment, due to massive state subsidy support, and second, aggressive state-backed diplomacy, marketing and in-country availability, which long went unchallenged by competitors from Europe, the US, Japan and South Korea. Across the global south in particular, ZTE and Huawei have secured exclusive rights as the countries "sole equipment supplier", allowing them to work with the government and telecom networks to create conditions for digital surveillance, repression and control.[21]

China's campaign for telco infrastructure extends beyond 5G equipment, to undersea and space-based aspects of Internet connectivity as well. Chinese companies have developed fibre optic cable networks in 70 countries and have been involved in at least 32 undersea cable projects in South East Asia.[22] Papua

To date, Chinese companies have signed more than 116 smart-city or safe-city partnerships, including 70 in BRI-participant countries and deals signed by Huawei in countries like Kenya, Singapore, Spain and Germany

[20] B. Dekker, M. Okano-Heijmans, and E.S. Zhang, *Unpacking China's Digital Silk Road*, Clingedael Report, Clingendael Institute, July 2020, p. 5.

[21] S. Feldstein, *Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Strategic Aims in Africa*, 8 May 2020.

[22] D.R. Russel and B.H. Berger, *Weaponizing the Belt and Road Initiative*, Asia Society Policy Institute, September 2020, p. 21.

New Guinea partnered with Huawei Marine to lay undersea fibre optic cables in the island nation, despite considerable political opposition from the US, Australia and Japan. Argentina and ZTE have entered into a fibre optic cable system agreement. In February 2021, China and Pakistan completed the PEACE fibre optic cable network connecting China to Europe through Pakistan and significantly reducing Pakistan's reliance on Indian Internet infrastructure.[23] The China-Myanmar International (CMI) terrestrial cable has been a key node in Chinese support to build out Myanmar's network coverage, with the focus on Myanmar as a DSR connectivity bridge between East, South East and South Asia.[24]

In addition, through the Belt and Road Space Information Corridor, China is exporting a space Internet connectivity ecosystem, primarily to the Indo-Pacific. Its Beidou Navigation Satellite System (BDS) network is available to BRI-participating countries, as an alternative to GPS and Galileo. 30 BRI countries are connected. Together, China and Pakistan built the first Beidou base-station in the city of Karachi, as part of the "Space Silk Road".[25] With 40 satellites, Beidou has already outstripped GPS's 31 operational satellites and Galileo's 24. This satellite network is also a strong standard-setting vehicle. In 2016, the State Council called the Beidou satellite network, the "digital glue" that would bind core infrastructure components of the BRI, such as ports and railways, to cities and smart manufacturing facilities – all premised on Chinese government intermediation.[26] The network would also create a protected extraterritorial communications ecosystem for the PLA, inoculated against GPS dependency.

---

[23] M. Haq, "China builds Digital Silk Road in Pakistan to Africa and Europe", *NikkeiAsia*, 29 January 2021.

[24] S.Rajaratnam School of International Studies (RSIS), "China's Digital Silk Road: The Integration of Myanmar - Analysis", *Eurasia Review*, 30 April 2019.

[25] S. Siddiqui, "BRI, BeiDou and the Digital Silk Road", *Asia Times*, 10 April 2019.

[26] D.R. Russel and B.H. Berger (2020), p. 21.

To date, Chinese companies have signed more than 116 smart-city or safe-city partnerships, including 70 in BRI-participant countries and deals signed by Huawei in countries like Kenya, Singapore, Spain and Germany. Safe-city solutions, built around AI-powered surveillance, big data processing, facial recognition and traffic and sewage management, have been a means of exporting China's "sharp eyes" approach to high-tech urban policing. Interestingly, the region with the highest concentration of Chinese-built smart-city projects is Europe.[27] China's suite of off-the-shelf urban management technologies not only automates public services, but also yields massive amounts of rich data. All of this data could be subject to intelligence service collection based on laws currently on the books. Sensetime, a Chinese AI-powered facial recognition specialist, announced a US$1 billion deal to build an AI research park in Malaysia, focusing on autonomous driving, health, education and smart-city ecosystems, with a view to establishing "AI governance" principles in the country.[28] Many of these projects, however, exist primarily on paper. In Germany, for instance, the Huawei-planned smart city in Duisburg, an industrial city with the world's largest inland port, which is also seen as a DSR endpoint, has largely stalled.[29]

A China-centric connectivity ecosystem would be sourced end-to-end with each component of physical Internet infrastructure, including copper and fibre cables, 5G equipment, satellite networks and mainframe computers for data processing, AI and cloud services. One underexplored aspect is normative capture. Third-country market adoption

[27] J. Kynge, "From AI to facial recognition: how China is setting the rules in new tech", *Financial Times*, 7 October 2020.

[28] GCR Staff, "China's SenseTime to help build $1bn AI park in Malaysia", *Global Construction Review*, 30 April 2019.

[29] M. Verfürden, "Duisburg will 'Deutschlands China-Stadt' sein – doch Jobs fehlen und die Zeit läuft ab" ("Duisburg wants to be Germany's China-city - however jobs are missing and time is running out"), *Handelsblatt*, 9 February 2021.

has an acculturating effect. Usage can necessitate implicit agreement, through contracts and terms of use, and create tacit acceptance of Chinese-centric conditions. Normative change can be hard to dislodge, given technological lock-ins and the effect of latent socialisation that comes through everyday use.

Technology becomes the heart of the BRI

The DSR gradually moved into the mainstream of China's efforts to promote outbound China-led development. Four factors contributed to this

By 2017, the political prioritisation of the DSR had risen, as senior CCP and government officials consistently emphasised the BRI's digital component. The DSR gradually moved into the mainstream of China's efforts to promote outbound China-led development. Four factors contributed to this.

First, the Chinese state and the CCP began to shift emphasis away from state-led ICT import substitution towards international strategies, thus aligning domestic capabilities and objectives with international capabilities and objectives. This alignment began to take shape in a subsequent series of plans addressing sectoral and policy issues, each with significant ICT subsets. At least 16 countries have signed MOUs relating to the DSR, but participant structure is less state-centric and can be less formal than the BRI. Up to 138 countries have an active DSR project.[30]

Second, even before 2020, public sentiment in BRI recipient countries was often hostile. Highly visible use of Chinese labour in countries where employment was a political priority was resented by local populations. The Chinese financing of infrastructure projects that mainly funded Chinese construction and infrastructure companies was perceived as corrupt and as a pathway into onerous loan conditions that the US labelled a

[30] RSIS, "China's Digital Silk Road: The Integration Of Myanmar", *Eurasia Review*, 30 April 2019.

"debt trap".[31] This has been exacerbated by the deteriorating economic outlooks for many of the BRI's most debt-ridden client countries, such as Pakistan. Amid construction delays and debt overhang, the shift to high-tech projects and services has already displaced some rail and transportation projects.

Third, the DSR's more normative character gives it greater operational flexibility. In essence, DSR projects can operate as plug-ins sitting on top of the more formalised, state-driven BRI. That said, experts have identified three core objectives: 1) driving greater digital integration of China into partner markets; 2) promoting the development, modernisation and upgrading of BRI-participant partners, using Chinese technology and 3) creating new regional or sectoral ecosystems based on China-centred tech value chains that either lock Western actors out or force them into conformity.[32] China's industrial innovation base – a mix of SOEs, private Chinese tech champions and start-ups – have become the federated emissaries of Chinese services, infrastructure, standards and ultimately, governance.

Unlike the traditional core of the BRI, which generally focuses on capital-intensive infrastructure projects and can involve state-finance, insurance and large teams of often Chinese workers visibly active in the construction process, the DSR is a hybrid of federated projects. Some of these are large, such as 5G network infrastructure projects, but many involve smaller Chinese private-sector actors operating under a loose mandate. The DSR umbrella is a mutually reinforcing campaign to establish market access – and ultimately competitiveness – across telecommunications infrastructure, data centres, IoT, smart cities, e-payment systems and social media. In the data governance space, such infrastructure capacity-building creates conditions for setting rules on enabling content moderation, filtering, data localisation and surveillance. Even when the state/CCP demands on Chinese companies are dormant, they

[31] A. Han and E. Freymann, "Coronavirus Hasn't Killed Belt and Road", *Foreign Policy*, 6 January 2021.

[32] B. Dekker, M. Okano-Heijmans, and E.S. Zhang (2020), p. 4.

remain present and can be activated through a thicket of laws and power relationships.

Lastly, the role of ICT technical standards and Internet governance is a central feature of the DSR. The CCP's desire to repatriate ICT standard-setting has long been an ambition of China's approach to the Internet. China's experience with TD-SCDMA and WAPI was telling. There is a well-known Chinese saying that third-tier companies make products, second-tier companies make technologies and first-tier companies set standards. But the integrated logic of the DSR aims to concentrate all three within the Sino-centric system.

The Standards Administration of China (SAC) established a dashboard to assist in the use and comparison of Chinese national standards, as part of its capacity building to create greater alignment with BRI-participating countries.[33] Currently, it has 85 agreements with more than 49 countries. In its 2019 Standardisation Development report, China listed technology standards exports as a BRI priority. SAC has explicitly shifted its focus from standard-setting cooperation with the United States and Europe to a greater emphasis on the Global South, with regionalised interest in Asia. China has fuelled discussion of a potential Asian Standardisation Organisation – a China-centric regional standard-setting body akin to the Asian Infrastructure Investment Bank – that would anticipate and feed up to ISO and IEC positioning it upstream of the global standard-setting process. The DSR exports technical standards and Internet governance models, reinforced through on-the-ground adoption of technologies that create path dependencies in user behavior.

Equally important, China has made a concerted effort to build capacity and influence in the multilateral standard-setting community. In 2013, it joined Germany, France, the US, Japan and the UK as a permanent member of the ISO Council.[34]

---

[33] P. Triolo et al., *The Digital Silk Road: Expanding China's Digital Footprint*, Eurasia Group, April 2020, p. 12.

[34] Embassy of the People's Republic of China in the Republic of Liberia, "China

From 2015-18, the ISO's President was a Chinese national. In 2020, the electrotechnical standard-setting body IEC, appointed a Chinese national, Yinbiao Shu, as President. Zhao Houlin, the Chinese national heading the UN's International Telecommunications Union (ITU), has been unabashed in his defence and support for BRI, Huawei and the DSR. The China Electronics Standardization Institute (CESI) leads the ISO working group on AI standards.[35] Chinese high-voltage grid standards are currently under consideration for the IEC's Global Energy Interconnection standards which, if adopted, would help to consolidate Chinese leadership in grid infrastructure.[36]

DSR in the Year of the Rat: Covid-19 and Changing Trends in Chinese Tech Foreign Policy

In many ways, the DSR accelerated during the Covid-19 crisis. The jolt to digital adoption drew new technological dependency into the spotlight, as platform services – such as video-conferencing and streaming services, e-commerce, social media, gaming, cloud-supported logistics and health tech – are all reliant on telecommunications infrastructure. At the same time, it fuelled a massive purchasing increase in smartphones, computers and IoT in the Global North. The hardware demand spike, in conjunction with decreased semiconductor production and greater awareness of supply chain vulnerabilities, fuelled new tensions in the China-US tech competition and created new urgency for Europe to pursue indigenous technological capabilities.

Against this backdrop, four broad trends can be identified in DSR development in the Covid-19 era. Each has nuances.

---

becomes ISO permanent member", 17 October 2018.

[35] https://sg.news.yahoo.com/china-aims-strengthen-ductor-supply-065031004.html

[36] J. Kynge and Nian Liu, "From AI to facial recognition: how China is setting the rules in new tech", *Financial Times*, 7 October 2020.

None reflects a complete shift in the characteristics that defined the broadly eclectic and differentiated DSR in the years prior to 2020. However, certain trends are noticeable and worthy of further exploration. Each of them expands the scale and scope of the DSR beyond what was originally envisaged, and certainly far beyond current perceptions and expectations regarding its deep and massive impact on China's rising influence both abroad and at home. While this section will draw on global data and information, the primary focus will remain on Europe.

Beyond hardware: Digital services, digital health, and FinTech

Covid-19-driven debt accumulation in middle- and low-income countries could slow demand for BRI-based infrastructure projects, making it more difficult for China to knit itself to partner states that then absorb excess Chinese capacity and labour

On connectivity and 5G infrastructure, the picture has been mixed. The threat of a US-China tech-stack split – combined with the economic uncertainty around Covid-19 and changing perceptions of China's intentions – have prompted countries to hedge their ICT infrastructure roll-out. The uncertainty overhang has been compounded by the US Entity List designation, and the 5G trustworthy equipment standards currently under development have changed the calculus of some countries, which do not want to get caught in the crossfire centred on Huawei. Japan, Australia, the United States and others have barred Huawei 5G equipment from their networks and raised concerns about cyber threats relating to back doors, service disruption and data manipulation.

Some predict that Covid-19-driven debt accumulation in middle- and low-income countries could slow demand for BRI-based infrastructure projects, making it more difficult for China to knit itself to partner states that then absorb excess Chinese capacity and labour. China's pattern of loan extension – rather than forgiveness – has proven a stumbling

block for large BRI-related infrastructure projects, including in telecommunications and connectivity.[37] For instance, the US has created new financing instruments, specifically the International Development Finance Corporation (DFC), to provide alternative financial support, including labour and environmental standards, to counter Chinese loans, including for connectivity infrastructure. In January 2021, the DFC provided Ecuador with the financial resources to pay back Chinese debt in exchange for guarantees to avoid Huawei and ZTE in its 5G infrastructure.[38]

In Europe, while efforts remain uneven, the EU's 2020 Toolbox Of Risk Mitigating Measures for Cybersecurity of 5G Networks has led to some degree of convergence on trustworthy standards for network equipment in mobile carrier infrastructure. Combined with the US Clean Network Initiative, the effect has been to narrow the space somewhat for usage of Huawei and ZTE equipment in Europe's 5G core and RAN networks. Countries like Romania, the Czech Republic and the Baltic states have deep security ties to the United States and have come under considerable pressure to ban Chinese equipment providers. Others, like the UK, France and Italy, have made a U-Turn away from Huawei sourcing, given the acute cybersecurity concerns, compounded by Chinese behaviour during the Covid crisis. Others again, such as Hungary, have been more open to Chinese connectivity and tech infrastructure. In a fourth category, Greece has tried to strike a delicate balance between the US and China on Huawei, in light of the changing security landscape in the Eastern Mediterranean. Greece signed on to the American 5G Clean Network, but it remains unclear what the Clean Network means to Greece and its acquisition intentions.[39] Serbia did

[37] K.M. Sutter, A.B. Schwarzenberg, and M.D. Sutherland, "China's "One Belt, One Road" Initiative: Economic Issues", Congressional Research Service, 22 January 2021.

[38] Ibid., p. 2.

[39] E. Gkritsi, "Huawei in Greece: How Snowden shaped EU's approach to

likewise, but at the same time uses thousands of Hikvision AI-powered surveillance cameras in Belgrade.

Globally, the picture has become more politically sensitive for Huawei and ZTE as well, although not always leading to declines in market share. The Blue Dot Network between Japan, Australia and the US creates similar certification mechanisms for connectivity infrastructure, among other things.[40] At the same time, reliance on Chinese 5G vendors has also grown in some places. For instance, 11 telcos in Gulf Cooperation Countries (GCC) signed massive 5G contracts with Huawei, as the oil-rich Middle East became increasingly tied economically to Chinese growth during the Covid crisis.

The geopolitics surrounding Huawei have also impacted on China's rise as a smartphone power. Chinese smartphones made up 60% of market share in ASEAN in 2019 and 25% in Europe. The hit to the Huawei brand – combined with chip shortages resulting from US Entity List Designations – has affected the company's global market share, with sales of Huawei smartphones declining from 18% of the global market in Q3 2019 to 8% in Q4 2020. It would be a mistake, however, to associate Huawei's geopolitically-driven decline with an overall hit to Chinese dominance in smartphones. Other Chinese smartphone makers – Xiaomi, Oppo, realme, Transsion and Vivo – have absorbed most of Huawei's share. In Europe, Xiaomi and Oppo took a major bite out of both Huawei and Samsung in 2020.[41]

The user base for China's data-intensive platforms and digital services remains largely limited to China, their data sets lack the diversity of data pools held by US technology companies

Even as the demand for Chinese ICT hardware has hit some headwinds, Chinese digital services have flourished. Because the user base for China's data-intensive platforms and digital

Huawei", *technode*, 21 January 2021.

[40] U.S. Department of State, "Blue Dot Network", 2021.

[41] A. Walker, "Xiaomi, not Samsung or Apple, is taking advantage of Huawei's woes in Europe", *Android Authority*, 1 March 2021.

services remains largely limited to China, their data sets lack the diversity of data pools held by US technology companies. China only has 20% of the cross-border data flows that the US has.[42] That has started to change, as both Chinese hardware and OTT (Over The Top) offering become available outside of China. TikTok was 2019's second-most downloaded app globally,[43] and shot up to number one in 2020, with more than 100 million active users in Europe.[44] The Covid-19 crisis has also been tied to growth in usage of AliExpress, including across some areas of Europe. Today it stands as the leading non-homegrown e-commerce platform in multiple countries throughout Europe, particularly in Central Europe and the Balkans. WeChat adoption outside of China remains insignificant. But the company is focused on expanding the ecosystem in China's Asian perimeter.

The Covid-19 crisis has also brought with it increased demand for sophisticated AI-powered digital health surveillance and diagnostics equipment. China has been maximalist in its deployment of health surveillance in the crisis and its companies subsequently became exporters.[45] China's use of a QR health code system for tracking and sharing travel and interaction authorisations became a mainstay of the country's management of the spread of Covid-19 within the country. Early in the pandemic, similar QR code certifications were in development to allow for cross-border tracking and verification as a component of travel, accommodation and restaurant booking systems across East Asia.[46] Alibaba offered its cloud services to host-countries early in the pandemic, to model and

[42] J. Woetzel et al. (2019), p. 3.

[43] A. Freer, "TikTok was the most downloaded app of 2020", *Business of Apps*, 15 December 2020.

[44] J. Firsching, "TikTok Statistiken 2020: 100 Mio. Nutzer in Europa & über 800 Mio. weltweit" ["TikTok Statistics 2020: 100 Mio. Users in Europe and over 800 Mio. worldwide"], *Future BIZ*, 15 September 2020.

[45] K. Sahin et al. (2020).

[46] Li Bo, "The Digital Belt and Road program yields fruits amid the coronavirus pandemic", *Beijing Review*, 14 May 2020.

track regional transmission patterns. Moreover, China has proposed to export its Corona Apps globally. With access to all data stored on smartphones, the Chinese Corona App has been cited as a proto-authoritarian governance tool providing the nascent basis for social scoring systems in countries like Saudi Arabia.

Chinese AI-powered diagnostic equipment has become standard across hospitals in middle-income countries like Ecuador.[47] Biotech companies, like the Beijing Genomics Institute, have offered to provide Covid-19 testing in other countries for free, as a means of collecting DNA data.[48] Efforts by groups like the Beijing Genomics Institute (BGI) have included genetic data collection even in places like the United States. Adding DNA data to a data profile stack that includes personal information, such as financial, insurance and employment data, could provide a powerful body for AI/ML training and analysis.

In Europe, AI-powered health surveillance tools have also increased. This is not insignificant, in view of the divergences in this area between Europe and the United States. For instance, the US added a number of facial recognition technology makers, such as Hikvision and SenseTime, to the Entity List on security and privacy grounds, as well on the grounds of their role in Xinjiang detention camps. But the European Union – a leading proponent of data protection – has deployed Hikvision biometric video technology at European institution entrances in order to monitor for Covid-19 symptoms.[49] Other biometric surveillance technology produced by companies like Dahua has also seen increased attention to their usage during the crisis.

---

[47] J. Kurlantzick, "China's Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom?", *The Diplomat*, 17 December 2020.

[48] G. Myre, "China Wants Your Data - And May Already Have It", *npr*, 24 February 2021.

[49] C. Sebastiani, "Open letter: Are the cameras and scanners used at the entrances of the Commission and EP buildings …", *Renouveau & Démocratie*, 11 November 2020.

A high rate of mobile payment adoption will concentrate financial transactions through Chinese based fintech gatekeepers. E-payment adoption could leapfrog purchasing behaviour in the EU and other Western countries. 95% of Chinese consumers already use mobile payment technology, compared to 64% globally and 24% in the United States. The 2019 value of Chinese digital transactions was more than that of the US, Japan, the UK, Germany and France combined.[50]

Lastly, China's rapid domestic adoption of payment systems is driving standard-setting on payment verification, dual offline technology, tax avoidance, money laundering and financial surveillance. It has also become a new front line for the government to assert control over fintech, in order to rein in financial, political and national security risk. Digital currency could be a key element of the DSR, by providing greater control of the monetary system layer in e-wallet transactions that can both enhance – but also tighten control on or circumvent – Chinese intermediary e-payment applications like WeChat Pay, Aliexpress/AliPay and a broad class of smaller lending platforms. The e-yuan will tighten centralised control of monetary transactions in the hands of the Chinese state within the "digital RMB-zone". Adoption would provide the People's Bank of China with the capability for real-time monitoring of global RMB-denominated transactions. It would also facilitate the displacement of the dollar as a global exchange currency and help lock in the RMB as a means of international exchange within DSR ecosystems.

Beyond tech transfer: Investments and acquisitions

There has also been an accelerated move towards Chinese Big Tech acquisitions of key external technology companies as a primary vector for gaining IP, market share and human capital in key technology sectors. This has long been true in

[50] J. Kynge and Sun Yu, "Virtual control: the agenda behind China's new digital currency", *Financial Times*, 17 February 2021.

the e-ecommerce space, but is increasingly the case in other areas as well, particularly fintech and gaming. Alibaba acquired Myanmar's largest e-commerce platform and the Myanmar Payment Union; took a US$1 billion stake in Indonesia's e-commerce champion, Tokopedia; and bought a controlling stake in Lazada, South East Asia's largest e-commerce platform with strengths in Malaysia and Singapore.

In Europe, the M&A trend in Over The Top (OTT) platforms has also accelerated since 2019. Tencent has been an investor in the German mobile banking platform, N26. Didi invests in the Estonian ride-sharing unicorn, Bolt. In the gaming industry – the hidden incubator for key strategic technologies like AI and augmented reality/virtual reality (AR/VR) – Tencent has gobbled up Europe's champions like the Finnish SuperCell in 2019 and the Czech Bohemia Interactive in 2020.[51] Offshoot strategic benefits remain unrecognised. After all, artificial intelligence would not have been possible had the demand for killer graphics spawned a Graphic Processing Unit (GPU) boom in the 1990s.[52] Tencent has joined with major Silicon Valley investors like Andreessen Horowitz and has focused on an acquisition strategy in social media and gaming.

Partnerships with foreign firms allow Chinese companies to deploy more rapidly, often leveraging higher quality technology from partners and benefiting from the added credibility, reputational advantages and geopolitical certainty that international partners bring, even as DSR comes under more intense international scrutiny. Alibaba has focused on a fast growth strategy, relying more on strategic partnerships with on-the-ground infrastructure, such as BT Cloud in the UK and SK Group in South Korea, to ramp up its overseas presence more quickly. This is partly intended to quickly create the enabling infrastructure for Chinese tech services, as they

[51] N. Watanabe, T. Wakasugi, and N. Matsumoto, "Tencent uses game business to expand global empire", *Nikkei Asia*, 23 January 2021.

[52] R. Toews, "Artificial Intelligence Is Driving A Silicon Renaissance", *Forbes*, 10 May 2020.

expand outside China, and avoid data localisation challenges. Thus far, AliCloud has more than 22 data centres abroad.[53]

Beyond outbound DSR: "Reverse-Flow" DSR

Even within China, questions have arisen as to whether investing in massive infrastructure projects along the BRI is sound, given the Covid-19 climate of financial risk. Many Chinese companies, particularly ICT state-owned and state-adjacent enterprises, have turned towards greater investment and consumption at home. Even as the first wave reached its peak in China itself, the CCP Politburo's Standing Committee called for accelerated 5G network development. China Mobile, China Telecom and China Unicom set themselves the task of establishing 550,000 5G base-stations by the end of 2020 as part of the country's Covid-19 recovery stimulus plan. This boosted domestic investment and the state's confidence in its capacity to monitor, control and capture.

In March 2021, Beijing announced the pledge to gradually lift certain foreign investment restrictions covering the telecommunications industry.[54] As part of its dual-circulation model, the Ministry of Industry and Information Technology's decision is a demonstration of greater confidence in China's capacity to control critical technological choke-points within its domestic production, while further integrating its telecommunications sector into the global ICT supply chains on China's terms. The logic behind this liberalisation of FDI also underscores China's negotiation of the Comprehensive Agreement on Investment (CAI) with the EU. Under the deal, the EU gains greater access to invest in the broader ecosystem around smart manufacturing. Manufacturing accounts for 50% of EU FDI in China, the majority of which is concentrated in the automotive industry.[55] As manufacturing and automotive

[53] P. Triolo et al. (2020), p. 12.

[54] "Plan to open telecom sector a bold move", *China Daily*, 5 March 2021.

[55] Z. Keck, "Outrage Over NSA Spying Spreads to Asia", *The Diplomat*, 31

move towards smart, systems-based operations – where data centres play a key role – the EU automotive sector will become more embedded in the DSR ecosystem, once tech-driven consumption and the thirst for ICT infrastructure upgrades pick up in key DSR markets.

In that sense, the EU's CAI with China should be viewed within the context of the DSR. This is particularly true of Germany, which held the EU Presidency at the time of the CAI negotiation's conclusion. Germany was already too dependent on China's massive market for it to emancipate itself from its reliance on Chinese consumers, a reality only accentuated by China's post-Covid economic snapback. China accounts for 40% of VW's global sales in China.[56] But as Germany's reliance on China grows, Germany's industrial base could be more closely grafted to China, in a fusion of systems governing smart cities, autonomous vehicles and manufacturing.

It is possible that the CAI could support the gradual incorporation – i.e. lock-in – of European manufacturing into the Chinese digital ecosystem, making it a point of leverage for DSR objectives globally. Siemens Advanta developed its Smart City digital hub in Hong Kong and is supporting DSR projects on advanced manufacturing, energy infrastructure and facilities managements in South East Asia. Baidu's move into autonomous vehicles focuses on its open-source Apollo platform and partnerships with Daimler on road navigation, voice command, sensors and visual recognition technology.

Beyond standard setting: Regulatory mirroring and global governance

Technical standard setting continues to remain at the heart of China's quest to establish greater control within the DSR space. For instance, amid the acute semiconductor crisis in 2021, the

October 2013.

[56] K. Ulrich, "Are German carmakers too dependent on China?", *Deutsche Welle*, 27 December 2020.

China Electronics Standardization Institute (CESI) launched a new semiconductor standardisation committee in order to formalise end-to-end control over its chip industry in the medium term.

China is aware that if its AI and other technology is perceived as under-regulated and authoritarian, its data-driven technology could be locked out of key countries, particularly in Europe

At the same time, heightened US-China tensions amid the Covid crisis have triggered new impulses in digital regulatory diplomacy geared towards states caught between the two tech superpowers. China is aware that if its AI and other technology is perceived as under-regulated and authoritarian, its data-driven technology could be locked out of key countries, particularly in Europe. In 2019, China stepped up its efforts to mirror Europe's digital regulatory discourse – on the market power of tech giants and data protection – in an effort to mollify international narratives of conflict, while at the same time consolidating the absolutist power of CCP rule at home. The US antitrust investigations and the introduction of the Digital Markets Act, examining the market power of tech platforms, coincided with China's moves against Ant Group, the Alibaba affiliate, which was blocked from going public in October 2020, and has increased Big Tech scrutiny on competition as a means of tightening state control on increasingly internationalised champions like Alibaba and Tencent. China's 2021 Blocking Statute – which invalidates extra-territorial sanctions in China – was explicitly modelled on the EU law in order to prevent Chinese Big Tech from complying with sanctions in other powers like Europe, where these companies are growing players.[57]

But perhaps the most evident area of increased sophistication and focus is data governance. As a counter-offensive to the US Clean Network Initiative, the Chinese Foreign Ministry

[57] K. Austin et al., *China's 'Blocking Statute' – New Chinese Rules to Counter the Application of Extraterritorial Foreign Laws*, Gibson Dunn, 13 January 2021.

launched its Global Data Security Initiative.[58] The diplomatic initiative aims to reinforce the notion of cyber sovereignty, while critiquing the perceived hypocrisy and bullying of the US in data access for intelligence (Snowden) and law enforcement (the CLOUD Act). Coupled with China's domestic push for a Personal Information Protection Law (PIPL) – which plays on the rhetoric of GDPR but in fact tightens state control over data *vis-à-vis* the private sector – the diplomatic effort at a new personal data order is aimed at appealing to Europeans, particularly Germans. Both efforts were launched immediately prior to the first high-level EU-China Digital Dialogue. This does not mean that Beijing is adopting the spirit of data protection centred on the notion of informational self-determination. China is not a party to APEC's Cross-Border Data Privacy Rules and has made no effort to achieve adequacy with the European Commission under the EU's data protection rules. In fact, the Chinese state is bank-rolling a tool to support Bytedance and WeChat in circumventing Apple's rules on privacy and user consent for data collection.[59]

Moreover, China is inching its way ever closer to the centre of digital multilateralism. Several UN agencies – including the UN Center for Trade Facilitation and Electronic Business and the ITU – have adopted the language supporting the DSR as a development avenue. As part of the UN's 2030 sustainable development agenda, the UN and China announced at the 75th General Assembly of the United Nations that they would set up two UN Data Centers in China – one focused on geospatial information and technology to be located in Deqing and a second UN Center on Big Data research to be located in Hangzhou. Both centres are less than an hour's drive from each other in Zhejiang. By wrapping these two strategically important, dual-use data classes in multilateralism, the Chinese

[58] Ministry of Foreign Affairs of the People's Republic of China, "Global Initiative on Data Security", 9 August 2020.

[59] P. McGee, "China's tech giants test way around Apple's new privacy rules", *Financial Times*, 16 March 2021.

government can lean on the UN's legitimacy when approaching third countries to provide data access in areas with evident and highly sensitive military potential.

Post-Covid-19 Outlook and Lessons for Europe

Like the US, China views technology as the necessary foundation of global power. Covid-19 has driven a reinvention of the DSR to focus more on M&A, health, fintech and digital services, and ICT adoption through domestic tech upgrades and new models of tech governance. The crisis has also helped to unwind the BRI's dependency on finance-intensive infrastructure projects at a moment when BRI recipient countries are coming under strain from the Covid-19 economic slowdown.

But the shift to a tech-centric BRI bumps up against the priorities of China's global competitors, particularly the United States, but increasingly the EU's geopolitical Commission and key Member States. Like other actors, the EU is increasingly aware that it could get caught in the crossfire – forced to choose between access to the Chinese market or US technology. The notion of technological decoupling from China or the United States is not an option for Europe. Europe is too dependent on China's massive market for it to emancipate itself from its reliance on Chinese consumers, a reality only accentuated by China's post-covid economic snapback and the reverse-flow DSR. Yet as its technological power grows, China's approach to technology has become more confident, belligerent, untrustworthy and ideologically incompatible with the European political system. Conversations in Brussels, Berlin and other capitals have become more pointed, as leaders ask to what extent Europe's accommodation with China on technology could ultimately help to midwife China's authoritarian dominance.

The EU is increasingly aware that it could get caught in the crossfire – forced to choose between access to the Chinese market or US technology

Europe's quest for digital sovereignty must address the DSR and Chinese techno-authoritarianism more directly. While American Big Tech, the Trump Administration and the general deterioration of American democracy have driven a justifiable desire in Europe to hedge its bets, the recent era has engendered a structural imbalance in the EU's regulatory enforcement and industrial policy. This has been defined primarily by the EU's perception of US tech dominance as a threat, rather than China's increasingly important role as a digital player or the ideological clashes between democratic and authoritarian visions for the digital international system. As the DSR shows, a more balanced and global approach would better suit Europe's strategic interests.

This means EU member-states have begun to make more effective use of screening of Chinese investment in strategic tech,[60] by expanding it to areas like online gaming, social media and fintech. Second, the EU must rethink trade controls, both on dual-use exports and on market access for imports, particularly of AI-powered surveillance equipment used in smart cities, digital services and Chinese health tech. Third, the EU and its Member States must examine the degree to which European industry is drawn into the DSR by reverse flow, particularly at this moment of acute Covid-induced economic fragility. Fourth, the EU must look at how its regulatory discourse – on data protection, competition, taxation and content moderation – can be distorted and ultimately deployed to support techno-authoritarianism. Finally, the EU must step up its efforts to build a positive ICT infrastructure and digital services agenda in the Global South. Efforts to extend the Ellalink undersea cable system between Europe and Latin America, the EU's space-based Secure Connectivity Initiative and the creation of a Digital Connectivity Fund for joint projects show that the muscle-memory here is slowly building. Ultimately, Europe

[60] Germany, for example, blocked Chinese takeovers of German firms developing strategic technology, such as the satellite communications technology company, IMST, the toolmaker, Leifeld, and the power grid operator, 50Hertz.

must see the power element in digital competition as one that binds infrastructure and services with universal values, such as human dignity and data privacy.